Библиографические ссылки

1. Измеряя неизмеримое : E-xecutive [Электронный ресурс]. Режим доступа : http://www.e-xecutive.ru/career/adviser/340036/.

2. *Астахова Л. В.*, *Землянская О. О.* Методика оценки кадровых уязвимостей информационной безопасности организации на этапе приема сотрудника на работу // Вестн. УрФО. Безопасность в информационной сфере. М., 2013. № 1(7). С. 53–58.

ПРАВОВЫЕ ВОПРОСЫ ВНЕДРЕНИЯ НОВОЙ СИСТЕМЫ ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ ОБЕСПЕЧЕНИЯ ФУНКЦИЙ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ

А. Н. Комиссаров[1], *Е. В. Рухлова*[2]
([1] Курган, КГУ, smack4ever@mail.ru;
[2] Челябинск, ЮУрГУ (национальный исследовательский университет), rukhlova-ekaterina@yandex.ru)

В юриспруденции под термином «тайна связи» понимается ценность, обеспечиваемая правом на тайну связи. На сегодняшний день право на тайну связи считается составной частью прав человека – (естественных прав личности). В Российской Федерации право на тайну связи (переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений) гарантируется Конституцией Российской Федерации (ч. 2, ст. 23). Эта же статья Конституции закрепляет положение о том, что ограничение права на тайну связи допускается только на основании судебного решения.

Однако в последнее время наметилась определенная тенденция по внесению изменений, направленных на ограничение права на тайну связи, в нормативно-правовые акты, призванные регулировать общественные отношения в области информационной безопасности. Так, благодаря выложенной в сеть Интернет информации компанией «ВымпелКом» интернет-пользователи узнали о готовящихся изменениях в Правила применения оборудования коммутации и маршрутизации пакетов информации сетей переда-

чи данных, включая программное обеспечение, обеспечивающее выполнение установленных действий при проведении оперативно-розыскных мероприятий (СОРМ-3 – это комплекс технических средств и мер, предназначенных для проведения оперативно-розыскных мероприятий в сетях телефонной, подвижной и беспроводной связи и радиосвязи, который внедряется в соответствии с проектом приказа Минкомсвязи РФ с 1 июля 2014 г.).

Российская СОРМ, в отличие от ETSI и CALEA (аналогичных европейской и американской систем соответственно), позволяет уполномоченным службам самостоятельно (до суда) определить пользователя, которого необходимо поставить на контроль и самостоятельно осуществляет данный контроль, что идет вразрез со ст. 23 Конституции Российской Федерации. Однако в ст. 63 Федерального закона «О связи» оговаривается, что: «Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами». Федеральными законами предусматриваются следующие случаи:

1. В соответствии с п. 15 ч. 2 ст. 7 Федерального конституционного закона «О военном положении» допускается «введение военной цензуры за почтовыми отправлениями и сообщениями, передаваемыми с помощью телекоммуникационных систем, а также контроля за телефонными переговорами, создание органов цензуры, непосредственно занимающихся указанными вопросами».

2. В соответствии с ч. 2 ст. 91 Уголовно-исполнительного кодекса получаемые и отправляемые осужденными письма, почтовые карточки и телеграммы подвергаются цензуре со стороны администрации исправительного учреждения.

3. В соответствии с ч. 2 ст. 186 Уголовно-процессуального кодекса при наличии угрозы совершения насилия, вымогательства и других преступных действий в отношении потерпевшего, свидетеля или их близких родственников контроль и запись телефонных и иных переговоров допускаются по письменному заявлению указанных лиц, но при отсутствии заявления указанных лиц – по судебному решению.

4. В соответствии с п. 4 ч. 3 ст. 11 Федерального закона «О противодействии терроризму» на территории, на которой введен правовой режим контртеррористической операции, допускается введение контроля телефонных переговоров и иной информации, передаваемой по каналам телекоммуникационных систем, а также осуществление поиска на каналах электрической связи и в почтовых отправлениях в целях выявления информации об обстоятельствах совершения террористического акта, о лицах, его подготовивших и совершивших, и в целях предупреждения совершения других террористических актов.

Однако в соответствии с проектом СОРМ-3 помимо досудебного доступа к данным пользователя со сторон спецслужб операторы связи будут обязаны хранить трафик пользователя в течение 12 ч (СОРМ-2 не обязывает операторов к хранению трафика совсем), передавать в уполномоченные органы IP-адреса, логины от наиболее популярных интернет-сервисов (поисковых систем, социальных сетей), посещаемых пользователем, а также данные о местоположении пользователя (СОРМ-2 допускает контроль за действиями пользователя только по требованию уполномоченных органов).

Таким образом, проект СОРМ-3 напрямую нарушает ч. 1 ст. 49 Конституции Российской Федерации, закрепляющую принцип презумпции невиновности, и в результате его принятия (обсуждения по этому вопросу еще ведутся) ст. 23 Конституции России полностью теряет свой правовой смысл.

На фоне мировой истерии по поводу безопасности человечества, возникшей после 11 сентября 2001 г., правительства различных мировых держав принимают непопулярные и антиконституционные нормативно-правовые акты, призванные «обеспечить безопасность общества и государства». Однако на деле такие акты становятся политической уловкой для тотального контроля над населением. Как вскрывшаяся слежка АНБ за гражданами в Соединенных Штатах объясняется соображениями безопасности и предотвращением террористических акций, так проект СОРМ-3 Минкомсвязь объясняет необходимостью раннего выявления криминалистических элементов, однако, как показала ситуация в США, интернет-слежка не смогла предотвратить теракта в Бостоне. И в Российской

Федерации такого рода сбор и хранение информации, полученной операторами связи, приведут лишь к избыточной нагрузке обеспечивающей инфраструктуры провайдеров связи, а не к достижению основной заявленной цели (указанной выше).

ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ ЗАЩИТЫ ОБЪЕКТОВ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ И ТРАНСПОРТНЫХ СРЕДСТВ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

М. М. Лысых, Т. Ю. Зырянова
(Екатеринбург, УрГУПС)

Обеспечение транспортной безопасности – это одно из направлений стратегии развития транспортного комплекса Уральского региона до 2030 г.

В соответствии с Федеральным законом «О транспортной безопасности» № 16 от 09.02.2007 г. [1] обеспечение транспортной безопасности – это реализация определяемой государством системы правовых, экономических, организационных и иных мер в сфере транспортного комплекса, соответствующих угрозам совершения актов незаконного вмешательства.

Целями обеспечения транспортной безопасности являются устойчивое и безопасное функционирование транспортного комплекса, защита интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Акт незаконного вмешательства (далее АНВ) – противоправное действие (бездействие), в том числе террористический акт, угрожающее безопасной деятельности транспортного комплекса, повлекшее за собой причинение вреда жизни и здоровью людей, материальный ущерб либо создавшее угрозу наступления таких последствий.

Требования по обеспечению транспортной безопасности, согласно ст. 8 вышеупомянутого закона, являются обязательными для исполнения всеми субъектами транспортной инфраструктуры.